AMENDMENTS TO THE CLAIMS

1. (Original) In a computer system comprising a plurality of nodes interconnected for communication via a network, a method including acts of:

(A) capturing, in a data structure, a notification provided by a node on the network, the notification comprising at least a portion of a transmission by the node, the transmission describing a network event;

(B) identifying a data element within the notification;

(C) updating an index, based on the data element, with an indication of a location within the data structure where the data element is recorded.

2. (Original) The method of claim 1, wherein the act (A) further comprises storing the data structure in a non-volatile storage.

3. (Original) The method of claim 2, wherein the act (A) further comprises storing the data structure in a file system in the non-volatile storage.

4. (Original) The method of claim 3, wherein the file system is a hierarchical file system.

5. (Original) The method of claim 3, further comprising an act comprising classifying the notification based on the data element, and wherein the act (A) further comprises storing the data structure in the file system based on the classification.

6. (Original) The method of claim 5, wherein the data element comprises an IP address of the node.

7. (Original) The method of claim 1, wherein the data structure is a file.

8. (Original) The method of claim 2, further comprising an act of compressing the data structure.

9. (Original) The method of claim 2, further comprising an act of creating a digital signature for the data structure.

10. (Original) The method of claim 1, wherein the transmission comprises at least one of a SYSLOG message, an SNMP message, a NetFlow message and a TCP packet.

11. (Original) The method of claim 1, further comprising acts of:

(D) accessing the index to determine, based on the indication, the location of the data element within the data structure; and

(E) accessing the data element at the location.

12. (Original) The method of claim 1, further comprising an act of creating a summary based at least in part on a presence of the data element within the notification.

13. (Original) The method of claim 12, further comprising an act comprising accessing the summary to determine the presence of the data element within the data structure.

14. (Original) At least one computer-readable medium encoded with instructions which, when executed by a computer, perform a method in a computer system comprising a plurality of nodes interconnected for communication via a network, a method including acts of:

(A) capturing, in a data structure, a notification provided by a node on the network, the notification comprising at least a portion of a transmission by the node, the transmission describing a network event;

(B) identifying a data element within the notification;

(C) updating an index, based on the data element, with an indication of a location within the data structure where the data element is recorded.

15. (Original) The at least one computer-readable medium of claim 14, further comprising instructions defining storing the data structure in a non-volatile storage.

16. (Original) The at least one computer-readable medium of claim 15, further comprising instructions defining storing the data structure in a file system in the non-volatile storage.

17. (Original) The at least one computer-readable medium of claim 16, wherein the file system is a hierarchical file system.

18. (Original) The at least one computer-readable medium of claim 16, further comprising instructions defining classifying the notification based on the data element and storing the data structure in the file system based on the classification.

19. (Original) The at least one computer-readable medium of claim 18, wherein the data element comprises an IP address of the node.

20. (Original) The at least one computer-readable medium of claim 14, wherein the data structure is a file.

21. (Original) The at least one computer-readable medium of claim 15, further comprising instructions defining compressing the data structure.

22. (Original) The at least one computer-readable medium of claim 15, further comprising instructions defining creating a digital signature for the data structure.

23. (Original) The at least one computer-readable medium of claim 14, wherein the transmission comprises at least one of a SYSLOG message, an SNMP message, a NetFlow message and a TCP packet.

24. (Original) The at least one computer-readable medium of claim 14, further comprising instructions defining accessing the index to determine, based on the indication, the location of the data element within the data structure; and accessing the data element at the location.

25. (Original) The at least one computer-readable medium of claim 14, further comprising instructions defining creating a summary based at least in part on a presence of the data element within the notification.

26. (Original) The at least one computer-readable medium of claim 25, further comprising instructions defining accessing the summary to determine the presence of the data element within the data structure.

27. (Original) A system for monitoring activity occurring in a computer system comprising a plurality of nodes interconnected for communication via a network, the system comprising:

a capture controller, said capture controller capturing, in a data structure, a notification provided by a node on the network, the notification comprising at least a portion of a transmission by the node, the transmission describing a network event;

an identification controller, said identification controller identifying a data element within the notification;

an update controller, said update controller updating an index, based on the data element, with an indication of a location within the data structure where the data element is recorded.

28. (Original) The system of claim 27, wherein the capture controller further stores the data structure in a non-volatile storage.

29. (Original) The system of claim 28, wherein the capture controller further stores the data structure in a file system in the non-volatile storage.

30. (Original) The system of claim 29, wherein the file system is a hierarchical file system.

31. (Original) The system of claim 29, further comprising a classification controller, said classification controller classifying the notification based on the data element, wherein the capture controller stores the data structure in the file system based on the classification.

32. (Original) The system of claim 31, wherein the data element comprises an IP address of the node.

33. (Original) The system of claim 27, wherein the data structure is a file.

34. (Original) The system of claim 28, further comprising a compression controller, said compression controller compressing the data structure.

35. (Original) The system of claim 28, further comprising a signature controller, said signature controller creating a digital signature for the data structure.

36. (Original) The system of claim 27, wherein the transmission comprises at least one of a SYSLOG message, an SNMP message, a NetFlow message and a TCP packet.

37. (Original) The system of claim 27, further comprising:

an access controller, said access controller accessing the index to determine, based on the indication, the location of the data element within the data structure; and accessing the data element at the location.

38. (Original) The system of claim 27, further comprising a summary controller, said summary controller creating a summary based at least in part on a presence of the data element within the notification.

39. (Original) The system of claim 38, further comprising a summary access controller, said summary access controller accessing the summary to determine the presence of the data element within the data structure.

40-81. (Cancelled)

82. (Original) A system for monitoring activity occurring in a computer system comprising a plurality of nodes interconnected for communication via a network, the system comprising:

means for capturing, in a data structure, a notification provided by a node on the network, the notification comprising at least a portion of a transmission by the node, the transmission describing a network event;

means for identifying a data element within the notification;

means for updating an index, based on the data element, with an indication of a location within the data structure where the data element is recorded.

83. (Original) The system of claim 82, wherein the means for capturing stores the data structure in a non-volatile storage.

84. (Original) The system of claim 83, wherein the means for capturing stores the data structure in a file system in the non-volatile storage.

85. (Original) The system of claim 84, wherein the file system is a hierarchical file system.

86. (Original) The system of claim 84, further comprising means for classifying the notification based on the data element, wherein the means for capturing stores the data structure in the file system based on the classification.

87. (Original) The system of claim 86, wherein the data element comprises an IP address of the node.

88. (Original) The system of claim 82, wherein the data structure is a file.

89. (Original) The system of claim 83, further comprising means for compressing the data structure.

90. (Original) The system of claim 83, further comprising means for creating a digital signature for the data structure.

91. (Original) The system of claim 82, wherein the transmission comprises at least one of a SYSLOG message, an SNMP message, a NetFlow message and a TCP packet.

92. (Original) The system of claim 82, further comprising:

means for accessing the index to determine, based on the indication, the location of the data element within the data structure; and

means for accessing the data element at the location.

93. (Original) The system of claim 82, further comprising means for creating a summary based at least in part on a presence of the data element within the notification.

94. (Original) The system of claim 93, further comprising means for accessing the summary to determine the presence of the data element within the data structure.

95-108. (Cancelled)